REMARKS

Initially, in the Office Action dated July 21, 2004, the Examiner has rejected claims 1, 4, 14 and 11 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,825,891 (Levesque et al.) in view of U.S. Patent No. 5,958,053 (Denker). Claims 9, 10, 19 and 20 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Levesque et al. in view of Denker and further in view of RFC 2401 (Atkinson et al.).

Claims 1-20 remain pending in the present application.

35 U.S.C. §103 Rejections

Claims 1, 4, 14 and 11 (and Applicants assume claims 2, 3, 5-8, 12, 13 and 15-18 since the Examiner includes arguments for these) have been rejected under 35 U.S.C. §103(a) as being anticipated by Levesque et al. in view of Denker. Applicants have discussed the deficiencies of these references in Applicants previously-filed response and re-assert all arguments submitted in that response. Applicants respectfully traverse these rejections and provide the following additional remarks.

Regarding claims 1 and 11, Applicants submit that Levesque et al. does not disclose or suggest the limitations in the combination of each of these claims of, inter alia, prior to performing encrypting security processing on a payload of a packet, storing information corresponding to selected information normally included in a payload of the packet in a field in a header of the packet where the field is not subject to the encrypting security processing, the selected information including transport level information, the transport level information being usable by

intermediate nodes between said node and said another node in the packet switched network to provide value added services relative to the transmission. The Examiner admits that Levesque et al. does not disclose or suggest selected information including transport level information where the transport level information is useable by intermediate nodes between said node and said another node in the packet switched network to provide value added services relative to the transmission, as recited in the claims of the present application, but asserts that Denker discloses these limitations at col. 3, lines 25-59. However, as noted previously, these portions of Denker merely disclose the Syncookie method as disclosed in Fig. 2. In this method, a server's Initial Sequence Number is generated by the server as a cryptologic function based upon the client's Initial Sequence Number, the client's IP address, and a secret known only to the server. After receiving a message from the client, the server can immediately check if the incoming acknowledgement number matches the appropriate hash function output and, if so, then the acknowledgement must have come in reply to a send ACK message from the server and the server can therefore trust the client. This is not, prior to encrypting security processing on a payload of a packet, storing information corresponding to selected information normally included in a payload of the packet in a field in a header of the packet where the field is not subject to encrypting security processing, the selected information including transport level information usable by intermediate nodes between a sending node and a receiving node to provide value added services relative to the transmission, as recited in the claims of the present application. These portions of Denker do not disclose or suggest anything related to selected

information normally included in a payload of a packet, or the selected information being transport level information usable by intermediate nodes to provide value added services. These portions of Denker merely disclose details of the commonly known Syncookie method. Denker discloses checking an acknowledgement message (see col. 3, lines 41-45). This is not permitting access to selected information via a header, as recited in the claims of the present application.

In the "Response to Arguments" section of the Office Action, the Examiner asserts that the "port number" in Denker corresponds with "transport level information" as recited in the claims of the present application, and that "authentication by matching hash values" in Denker corresponds to "value added services" as recited in the claims of the present application. The Examiner (using Applicants' dependent claims) has merely picked single discrete words from Denker with no relation at all to the limitations in combination in the claims of the present application. Denker merely discloses the port number should be encoded using the Syncookie method. This is not information normally included in a payload of a packet, or prior to performing encrypting security processing on a payload of a packet, storing information corresponding to selected information normally included in a payload of said packet in a field in a header of said packet where said field is not subject to said encrypting security processing, or permitting access to said selected information normally included in said payload of said packet via said header of said packet. Denker does not disclose or suggest that the port number is normally included in a payload of a packet now being stored in a header of the packet, as recited in the claims of the present application.

Moreover, the Examiner's assertions fail for other reasons. The "port number" in Denker (and asserted by the Examiner as corresponding to transport level information) is not useable by intermediate nodes between a node and an another node in the packet switched network to provide "authentication by matching hash values" as disclosed in Denker and asserted by the Examiner as corresponding to value added services. The claims of the present invention recite transport level information being useable by intermediate nodes between said node and said another node in the packet switched network to provide value added services relative to the transmission. The Examiner provides no disclosure in Denker to support the assertion that "Denker discloses the transport information is used as a portion of a security authentication and thus provides a value added service such as policing", but appears to use Applicants' claim 2 to support these assertions. Denker does not disclose or suggest the limitations in the combination of each of claims 1 and 11 of the present application.

Regarding claims 2-8 and 12-18, Applicants submit that these claims are dependent on one of independent claims 1 and 11 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. For example, Applicants submit that neither Levesque et al. nor Denker disclose or suggest the selected information being stored in a security protocol header of the header of the packet, the security protocol header not being subject to the encrypting security processing, or value added services including differentiated services policing or metering, or transport level information including transport protocol information including TCP, UDP, ICMP, or port number information.

Accordingly, Applicants submit that neither Levesque et al. nor Denker, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 1-8 and 12-18 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 9, 10, 19 and 20 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Levesque et al. in view of Denker and Atkinson et al. The deficiencies of Atkinson have been discussed in Applicants' previously-filed response. Applicants respectfully traverse these rejections.

Applicants submit that claims 9, 10, 19 and 20 are dependent on one of independent claims 1 and 11 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. Applicants submit that Atkinson et al. does not overcome the substantial defects noted previously regarding Levesque et al. and Denker. For example, Applicants submit that none of the cited references disclose or suggest the encrypting security processing being performed according to the encapsulating security payload (ESP) or according to the authentication header (AH) protocol. Further, there would be no motivation for one of ordinary skill in the art to combine Denker, that relates to use of the TCP2B and TCP2E protocols with Atkinson, that relates to the use of AH and ESP protocols, since each reference teaches away from the other as there would be no motivation to combine conflicting protocols.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in

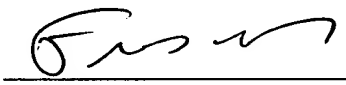
the combination of each of claims 9, 10, 19 and 20 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

In view of the foregoing amendments and remarks, Applicants submit that claims 1-20 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (referencing attorney docket no. 0173.37334X00).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 312-6600